FY11 PHYSICAL SECURITY ASSURANCE PLAN

March 2011

Revision 2

Approved By: Douglas M ____________________ Date: 3-28-11

Doug Fleming
Director, Environment, Health and Safety Division

Approved By: Dan Lunsford ____________________ Date: MARCH 22, 2011

Dan Lunsford
Group Leader, Security and Emergency Operations Group

RECORD OF REVISIONS

Revision #	Date	Description
1	February 2010	Revised to include: New Format Self-assessment sub topical ratings Justification and rationale for ratings Criteria to be addressed in initial, periodic and self assessment reports Root cause analysis, risk assessment and cost-benefit analyses of corrective actions resulting from findings in a survey or self-assessment.
2	March 2011	Revised to include: Updated activity schedule for Biennial Safeguards and Security Self Assessment, Peer Review of Biennial Safeguards and Security Self Assessment, Biennial DOE Security Survey.

CONTENTS

LAWRENCE BERKELEY NATIONAL LABORATORY (LBNL) PHYSICAL SECURITY ASSURANCE PLAN

1. Introduction

The Lawrence Berkeley National Laboratory (LBNL) Physical Security Assurance Plan is designed to ensure that LBNL physical security programs and processes meet contractual requirements, are effective, and support the LBNL mission. By implementing this Plan, LBNL will drive and sustain performance improvement by evaluating its programs and processes, self-identifying, correcting, and preventing issues. LBNL will use this Plan to demonstrate to the Department of Energy (DOE), the University of California (UC), and LBNL management that LBNL provides efficient, effective, and responsive Physical Security.

LBNL is a non-classified laboratory and is registered with the DOE as a Class C, Security Protection Level IV facility. There are a limited number of DOE security interests that are protected in five Property Protection Areas (PPA). The remainder of the site is a General Access Area (GAA) with an open research environment. The LBNL Physical Security program assures all visitors and employees of an open and secure work environment that fosters the continuation of creative scientific advances. Integrated security management ensures the protection of Laboratory assets, including physical and intellectual property, and establishes programs for physical and cyber security, export control, and counterintelligence.

2. Independent Assessment

2.1. DOE Berkeley Site Office

The DOE Berkeley Site Office (BSO) performs oversight activities to ensure physical security contract requirements are adequately defined and effectively implemented. Oversight is performed primarily through assessments and reviews throughout the fiscal year to support its annual evaluation of the Laboratory's physical security performance. Assessment topics are generally planned and calendared at the start of the performance year.

2.2. Biennial DOE Security Surveys

Pursuant to the Facility Data and Approval Report (FDAR) and DOE Manual 470.4-1, Program Planning and Management surveys of LBNL's security are performed biennially. LBNL is registered with DOE as a Property Protection facility with approval for the storage of category IV special nuclear materials. These Security Surveys are conducted by the DOE Office of Science (SC) Integrated Service Center at the request of the Berkeley Site Office (BSO). The surveys provide assurance to the Department of Energy and other government agencies (OGAs) that safeguards and security (S&S) interests and activities are protected at the required levels. Additionally, the surveys provide a basis for line management to make decisions regarding S&S program implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities.

2.3. DOE Office of Health, Safety, and Security (HSS)

The DOE Office of Health, Safety, and Security (HSS) provides DOE line management, Congress, and other stakeholders with an independent evaluation of the effectiveness of DOE policy and line management performance in safeguards and security; cyber security; emergency management; environment, safety and health; and other critical areas as directed by the Secretary.

On an as needed or requested basis, the DOE HSS conducts inspections and special reviews, and works in collaborative efforts such as Site Assistance Visits to assess crosscutting security issues.

2.4. Peer Review of the Biennial Safeguards and Security (S&S) Self Assessment

This peer review will focus on validation of the Biennial Safeguards and Security Self Assessment to provide feedback on performance and organization of LBNL's S&S activities in order to foster continuous improvement. This review will be conducted by security representatives from SLAC National Accelerator Laboratory and Sandia National Laboratory/California. Both of these laboratories conduct fundamental research that is funded by the Department of Energy and have security programs similar to those implemented at LBNL. This Peer Review will be completed by September 30, 2012.

3. Self Assessment

3.1. Triennial Site Security Risk Assessment

Pursuant to DOE M 470.4-1, DOE requires the conduct of risk assessments both in the safeguards and security planning process and as part of all project management and capital planning. The foundation of the graded approach is the use of the DOE Graded Security Protection (GSP) policy as a base line and the conduct of a local security risk assessment.

The LBNL SEO Group conducts Triennial Risk Assessments to provide graded protection in accordance with an asset's importance or the impact of its loss, destruction, or misuse. The results of the assessments, which also determine system effectiveness, are key considerations that are used by LBNL management in coordination with BSO to establish acceptable risk levels. As the laboratory and local threats change, the SEO group conducts updates.

3.2. Project Management Security Risk Assessment

DOE O 413.3A, Program and Project Management for the Acquisition of Capital Assets, outlines the requirements to perform Security Risk Assessments during project planning activities in order to identify potential security risks. Projects managed within DOE must have an integrated project team that includes participation by the security staff. The security staff is included in all planning phases of every major project to assure the identification of applicable safeguards and security requirements. The triennial Security Risk Assessment is performed every third July by the SEO Group with an independent consultant and/or a Safeguards and Security peer, typically from SLAC National Accelerator Laboratory and/or Sandia National Laboratory/California.

3.3. Biennial Safeguards and Security (S&S) Self Assessment

DOE M 470.4-1 defines LBNL's responsibility to perform self-assessments between the Security Surveys performed by the DOE to evaluate all applicable Safeguards and Security (S&S) program elements. This S&S Self-Assessment provides assurance to the LBNL Director and the Manager of the DOE BSO that S&S interests and activities are protected at the required levels. Additionally, it provides a basis for LBNL line management to make decisions regarding S&S program implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities.

This S&S Self-Assessment also incorporates an independent assessment element by enlisting a security consultant and/or peer security professionals to participate in the self-assessment activity.

The Self-Assessment is conducted in three phases:

1. Phase one focuses on planning and coordination between participating organizations
2. Phase two focuses on performance methodologies, such as document review, personnel interview and observation of processes or field locations
3. Phase three focuses on post assessment activities such as data validation and analysis; identification, risk assessment and causal analysis of findings, determining cost-benefit analysis of corrective actions and corrective action plan development.

S&S sub-topical elements may also be evaluated as part of the Self-Assessment. Applicable sub-topical elements at LBNL include Protection Program Management, Protective Force (Security Services Subcontractor), Physical Security, Personnel Security (Safeguards and Security Awareness), Unclassified Visits and Assignments by Foreign Nationals, Nuclear Materials Control and Accountability

The sub-topical elements that do not apply to LBNL are noted with a "D" on the DOE form 470.8, Survey/Inspection Report listed as attachment D.

The sub-topical element of unclassified cyber security is not rated (NR) in the physical security self assessment. The cyber security topical element is managed by the Information Technology (IT) Division.

4. Performance Measures

4.1. Performance Evaluation and Measurement Plan

The Performance Evaluation and Measurement Plan (PEMP) primarily serve as DOE's basis for review of the contractor's high priority outcome assessment for incentive fee and term extension. The performance evaluation provides a standard by which to determine whether the Laboratory is managerially and operationally in control of the Laboratory and is meeting the mission requirement and performance expectations/objectives of the Department as stipulated within the contract.

The PEMP appraisal process institutes a common structure and scoring system across all of the Office of Science laboratories. Structured around eight performance goals, the appraisal process emphasizes the importance of delivering the science and technology necessary to meet the missions of the DOE; of operating the Laboratory in a safe, secure, responsible and cost-effective way; and of recognizing the leadership, stewardship and value-added provided by the senior leadership of the Laboratory and UC. Input is solicited from all the major sponsors of work at the Laboratory. Goal 8, Sustain and Enhance the Effectiveness of Integrated Safeguards and Security Management (ISSM) and the Emergency Management System, includes physical security protection in one its objectives.

4.2. Physical Security Performance Measures

Performance Measures are structured to assess key physical security elements:

- Program planning and Management
- Physical Security
- Foreign Visits and Assignment
- Personnel Security

See Attachment B.

Physical Security performance indicators are managed within the SEO Group and are available upon request.

5. Reporting

5.1. Quarterly Assurance Report

Physical Security prepares a Quarterly Assurance Report for BSO, UCOP, and LBNL Management. Each Assurance Report provides an overview of LBNL performance and recent assurance activities, including activities detailed in the Physical Security Assurance Plan; performance against the PEMP's Goals, Objectives, and Notable Outcomes; and related activities. This report provides the basis for a quarterly tri-party Assurance meeting with counterparts from BSO and UCOP. Following meetings of each Operations' function, senior BSO, UCOP, and LBNL Management meet to discuss significant risks and concerns and corresponding mitigations.

5.2. Safeguards and Security Information Management System (SSIMS)

LBNL utilizes SSIMS for the registration of security interests; status of security surveys, findings and corrective actions; and reporting of security incidents based on Incident Measurement Index directed by DOE. The SSIMS is managed by DOE and input to the system is coordinated by the BSO through the DOE-Office of Science Integrated Service Center.

5.3. Occurrence Reporting and Processing System (ORPS)

The Department of Energy's Occurrence Reporting Program provides timely notification to the DOE complex of events that could adversely affect public or DOE worker health and safety, the environment, national security, DOE's safeguards and security interests, functioning of DOE facilities, or the Department's reputation. While this is primarily a safety oriented system, incidents that are security related may require dual reporting in both the ORPS and SSIMS systems. ORPS reporting is performed in accordance with LBID-2488, *LBNL ORPS Manual.*

6. Issues Management

6.1. Corrective Action Tracking System

Physical Security assurance activities include the utilization of the Laboratory's Issues Management Program (IMP). This program encompasses the continuous monitoring of work programs and performance to promptly identify issues to determine their risk and significance, their causes, and to identify and effectively implement corrective actions to ensure successful resolution and prevent the same or similar problems from occurring.

Issues are program and performance deficiencies, nonconformance, or findings that are identified through employee discovery, self-assessments, internal assessments or external reviews. These issues are managed according to the requirements of LBNL/PUB-5519 (1), *Issues Management Program Manual.*

All physical security issues and associated corrective actions (except for those that are immediately corrected or rectified) are entered into the LBNL Corrective Action Tracking System (CATS) database. CATS is an online tool used to identify, track, and resolve issues and their associated corrective actions as well as verify the implementation of those corrective actions. This database, accessible from anywhere in the world, enables LBNL employees to identify, track, manage, resolve, and search for issues and associated corrective actions.

All LBNL personnel are responsible for identifying issues that may require correction, improvement, or management attention for inclusion into the CATS database.

6.2. Data Monitoring and Analysis

Data Monitoring and analysis of security issues is performed to help monitor and analyze program and performance deficiencies, item characteristics and reliability, process implementation, and other quality-related information to identify items, services, activities, and processes needing improvement. These activities are performed in accordance with LBNL/PUB-5519 (3), *Data Monitoring and Analysis.*

7. Lessons Learned and Best Practices

A Laboratory-wide lessons learned and best practices program exists that provides a systematic approach towards continuous improvement. The SEO Group will develop and evaluate lessons learned and best practices and distribute them to appropriate parties. As appropriate, the SEO Group integrates lessons learned and best practices into the safeguards and security training program.

The SEO group utilizes a variety of activities to gain input and to share its operating experiences:

- Staff Meetings
- Web Based – Today at Berkeley Lab
- Focus groups
    - Locks & Keys
    - Foreign Visits and Assignments (FV&A)
    - Sensitive Subjects
- DOE Security Lessons Learned Center (SEC-LLC) [Managed for DOE by Los Alamos National Laboratory http://dns-lessons.lanl.gov/]
    - The center provides a repository and forum for sharing innovative new tools and practices to address common security issues, improve the efficiency of the security program, and help prevent security incidents.

ATTACHMENT A

Contractor Assurance System (CAS) Description and Physical Security Activities Crosswalk

CAS DESCRIPTION		PHYSICAL SECURITY ASSURANCE PLAN	
Section Description	**Section**	**Section Description**	**Section**
Assessment	3.3	Independent Assessment	2.0
Assessment	3.3	Self Assessments	3.0
Performance Metrics	3.4	Performance Measures	4.0
Continuous Improvement	3.6	Reporting	5.0
Issues Management	3.5	Issues Management	6.0
Issues Management	3.5	Corrective Action Tracking System	6.1
Issues Management	3.5	Lessons Learned and Best Practices	7.0

ATTACHMENT B

FY11 Laboratory Management Performance Measures for Physical Security

Performance Measures routinely monitored by LBNL management:
Program Planning and Management: a) Number of anomalies of the insensitive explosive materials program b) Number of anomalies of the controlled substances program

ATTACHMENT C

Consolidated Assessment Schedule

Assessment Title	Date Performed	Performed By
Triennial Site Security Risk Assessment	Triennial, scheduled for June 2011	SEO Group with independent consultant and/or S&S Peer
Project Management Security Risk Assessment	As needed for new construction	SEO Group
Biennial Safeguards and Security Self Assessment	Biennial, scheduled for September 2012	SEO Group
Peer Review of Biennial Safeguards and Security Self Assessment	Biennial, scheduled for September 2012	Security Representatives from SLAC and SNL/CA
Biennial DOE Security Survey	Biennial, last performed July 2011	DOE Office of Science Integrated Service Center

ATTACHMENT D

DOE Form 470.8
Survey/Inspection Report

DOE F 470.8
(05-05)
Replaces 5634.1 (05-94)
All Other Editions are Obsolete

U.S. Department of Energy

SURVEY/INSPECTION REPORT FORM

1. Survey Type: □ Initial □ Periodic □ Special □ Termination □ EPR □ NPR □ OA

2. Report #

3. Facility Name: The Regents of the University of California
Lawrence Berkeley National Laboratory

4. a. Facility Code: 141
b. RIS Code: DNA

5. Survey Date(s):

6. a. Findings: □ Yes □ No
b. Findings Against Other Facilities:

7. Composite Rating:

8. Previous Survey Date(s):

9. Unresolved Findings: □ Yes □ No

10. Previous Rating:

11a. Surveying Office: DOE ORO

11b. Cognizant Security Office:

11c. Other Offices with Interests:

12. Ratings:

a) PROGRAM MANAGEMENT AND SUPPORT

PROTECTION PROGRAM MANAGEMENT	
Program Management and Administration	
Resources and Budgeting	
Personnel Development and Training	
S&S PLANNING AND PROCEDURES	
MANAGEMENT CONTROL	
Surveys and Self Assessment Programs	
Performance Assurance Program	D
Resolution of Findings	
Incident Reporting and Management	
PROGRAM WIDE SUPPORT	
Facility Approval and Registration of Activities	
Foreign Ownership, Control or Influence	D
Security Management in Contracting	D
OVERALL RATING	

b) PROTECTIVE FORCE

MANAGEMENT	
TRAINING	
DUTIES	
FACILITIES AND EQUIPMENT	
OVERALL RATING	

c) PHYSICAL SECURITY

ACCESS CONTROLS	
INTRUSION DETECTION & ASSESSMENT SYSTEMS	
BARRIERS AND DELAY MECHANISMS	
TESTING AND MAINTENANCE	
COMMUNICATIONS	
OVERALL RATING	

d) INFORMATION PROTECTION

BASIC REQUIREMENTS	
TECHNICAL SURVEILLANCE COUNTERMEASURES	D
OPERATIONS SECURITY	D
CLASSIFICATION GUIDANCE	D
CLASSIFIED MATTER PROTECTION & CONTROL	D
Control of Classified Matter	D
Special Access Programs and Intelligence Information	D
OVERALL RATING	

e) CYBER SECURITY

CLASSIFIED CYBER SECURITY	D
Leadership, Responsibilities and Authorities	D
C&A, Risk Management and Planning	D
Policy, Guidance and Procedures	D
Technical Implementation	D
Performance Eval Feedback & Continuous Improvement	D
TELECOMMUNICATIONS SECURITY	D
UNCLASSIFIED CYBER SECURITY	NR
Leadership, Responsibilities and Authorities	NR
C&A Risk Management and Planning	NR
Policy, Guidance and Procedures	NR
Technical Implementation	NR
Performance Eval Feedback & Continuous Improvement	NR
OVERALL RATING	

f) PERSONNEL SECURITY PROGRAM

ACCESS AUTHORIZATIONS	D
HUMAN RELIABILITY PROGRAM	D
CONTROL OF CLASSIFIED VISITS	D
SAFEGUARDS AND SECURITY AWARENESS	
OVERALL RATING	

g) UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS

SPONSOR PROGRAM MANAGEMENT & ADMIN	
COUNTERINTELLIGENCE REQUIREMENTS	
EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS	
SECURITY REQUIREMENTS	
APPROVALS AND REPORTING	
OVERALL RATING	

h) NUCLEAR MATERIALS CONTROL & ACCOUNTABILITY

PROGRAM ADMINISTRATION	
MATERIAL ACCOUNTABILITY	
MATERIALS CONTROL	
OVERALL RATING	

13. Report Prepared by:
Date:

14. Report Approved by:
Date:

15. Distribution:

16. General Comments:

SURVEYS: S = Satisfactory M = Marginal U = Unsatisfactory D = Does Not Apply NR = Not Rated (SPEC only)
INSPECTIONS: EP = Effective Performance NI = Needs Improvement SW = Significant Weakness D = Does Not Apply